Deutscher Bundestag **Drucksache 17/6829**

17. Wahlperiode 23. 08. 2011

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Frank Tempel, Petra Pau, Jens Petermann, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 17/6757 –

Datenleck auf Servern von Ermittlungsbehörden

Vorbemerkung der Fragesteller

Mitglieder der sogenannten no-name-crew haben nach eigenen Angaben neben dem zentralen Server für das Observationsprogramm „Patras“ auch andere Server der Bundespolizei kompromittiert und heruntergeladene Dateien ins Netz gestellt. Diese Dateien sind teilweise noch verschlüsselt. FOCUS ONLINE hat am 16. Juli 2011 gemeldet, dass zumindest bei den Servern für das Observationsprogramm „Patras“ grundlegende Sicherheitsmängel den Diebstahl ermöglichten. Zahlreiche Server der Bundespolizei, der Zollverwaltung und der Landeskriminalämter sind daraufhin vom Netz genommen worden.

Laut dem Bundesvorsitzenden, Klaus Jansen, Bund der Kriminalbeamter, ist wegen der Kompromittierung von Bundespolizeiservern der Arbeitskreis II der Innenministerkonferenz zusammengetreten. Entgegen der Forderung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wurden weder Öffentlichkeit noch Parlament noch die Betroffenen selbst konkret über diese Datenlecks in hochsensiblen Bereichen und die dabei zugänglich gewordenen Daten informiert (vgl. Presseerklärung des BfDI vom 12. Juni 2011 „Informationspflicht muss auch für Datenschutzpannen bei Behörden eingeführt werden“).

Vorbemerkung der Bundesregierung

Die sogenannte No-Name-Crew hat am 7. Juli 2011, um 18.04 Uhr, in einem Bekennerschreiben an das Hamburger Abendblatt die Veröffentlichung von Daten der Bundespolizei angekündigt. Am 7. Juli 2011 gegen 23.40 Uhr erschienen auf der Webseite der „No-Name-Crew“ Softwarepakete und dazugehörige Anwendungshinweise sowie Einsatzdaten aus einem Zielverfolgungssystem „Paip-Tracking-Server“ (PATRAS). Mit diesem Geoinformationssystem können berechtigte Nutzer die Standorte der Zielverfolgungseinheiten (GPS-Tracking Units) feststellen und dokumentieren. Diese Geo-Daten sind mittels einer kartengestützten Webanwendung grafisch darstellbar.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 17. August 2011 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Die PATRAS-Server werden als abgesetzte Systeme im Internet getrennt von den Behördennetzen betrieben. Da zunächst nicht absehbar war, ob noch weitere Daten abgeflossen sind, wurde der Sachverhalt auf die Tagesordnung einer ohnehin angesetzten Telefonkonferenz des Arbeitskreises II der Innenministerkonferenz gesetzt.

Die forensische Untersuchung der abgeschalteten Server sowie der im Rahmen der Ermittlungen sichergestellten Daten dauert an. Nach derzeitigem Stand der Ermittlungen sind jedoch keine polizeilichen Netzwerke kompromittiert worden und keine Daten aus Ermittlungsverfahren abgeflossen.

1. Welche Arten von Dateien und Daten wurden in welchem Umfang von Servern der Bundespolizei und des Zolls von Mitgliedern der sogenannten no-name-crew entwendet?

Nach derzeitigem Stand der Ermittlungen handelt es sich um Geo-Daten sowie Steuerungsdaten für die Ortungstechnik aus einem Zielverfolgungssystem des Zollkriminalamtes (ZKA) sowie um Softwarepakete und Servicemitteilungen zur Installation von PATRAS-Servern der Bundespolizei, die ohne notwendigen Freischaltschlüssel nicht verwendet werden können.

2. Welche weiteren Sicherheitsbehörden waren gleichartigen Angriffen mit welchen Ergebnissen ausgesetzt?

Nach derzeitigem Stand der Ermittlungen kam es bei keiner weiteren Sicherheitsbehörde des Bundes zu einem erfolgreichen Angriff. Darüber hinaus sind nach derzeitiger Kenntnis der Bundesregierung vier Bundesländer gleichartigen Angriffen ausgesetzt gewesen. Die Bundesregierung hat zu diesen außerhalb ihres Verantwortungsbereichs liegenden Systemen der Bundesländer keine detaillierten Erkenntnisse.

3. Wie haben die Bundesregierung und die Sicherheitsbehörden von den Datenlecks Kenntnis erhalten?

Die „No-Name-Crew“ hat am 7. Juli 2011, um 18.04 Uhr, in einem Bekennerschreiben an das Hamburger Abendblatt die Veröffentlichung von Daten der Bundespolizei angekündigt. Durch das Hamburger Abendblatt wurde die Bundespolizei informiert, die wiederum das Bundesministerium des Innern und das Bundesamt für Sicherheit in der Informationstechnik über den Sachverhalt unterrichtete.

Das Zollkriminalamt erhielt die Meldung am 8. Juli 2011 um 1.35 Uhr von der Bundespolizei fernmündlich.

4. Wie viele laufende Ermittlungen bzw. laufende Verfahren sind potentiell betroffen?

5. Welche Auswirkungen haben nach Einschätzung der Bundesregierung die bisherigen Veröffentlichungen und potentielle weitere Veröffentlichungen der Dateien auf laufende Ermittlungen bzw. laufende Verfahren?

Nach bisherigem Ermittlungsstand sind keine Einsatzdaten aus dem Zielverfolgungssystem der Bundespolizei kompromittiert worden. Nach heutigem Stand sind keine Daten aus Ermittlungsverfahren der Bundespolizei abgeflossen. Aus

den Zielverfolgungsdaten der Bundespolizei lassen sich für Außenstehende keine Zusammenhänge zu Verfahren oder Ermittlungen herstellen.

Aus dem Bereich der Zollverwaltung sind zwar Geo-Daten entwendet worden, jedoch erfolgt eine Verknüpfung der Positionsdaten mit dem konkreten Ermittlungsverfahren durch die ermittelnde Dienststelle über andere – nicht mit dem Zielverfolgungssystem PATRAS verbundene – Informationssysteme, so dass grundsätzlich davon auszugehen ist, dass keine laufenden Ermittlungen der Zollverwaltung gefährdet sind. Darüber hinaus sind die zugrundeliegenden Ermittlungsverfahren überwiegend bereits abgeschlossen.

6. Welche Datennetze waren betroffen, und wie viele Server der entsprechenden Netze sind kompromittiert worden?

Die Ortungssysteme werden als einzelne Rechner im Internet außerhalb der Behördennetze betrieben. Da die vollständige Auswertung der sichergestellten Daten noch nicht abgeschlossen ist, können zum jetzigen Zeitpunkt keine abschließenden Angaben zum Umfang des Datenabzuges gemacht werden. Nach dem gegenwärtigen Stand der Ermittlungen ist es den Tätern nicht gelungen, die internen Netze und Datenbanken der Polizei und der Zollverwaltung zu kompromittieren. Die Angriffe blieben auf das von den übrigen IT-Anwendungen getrennte Zielverfolgungssystem beschränkt.

Die von der „No-Name-Crew“ zur Untermauerung ihrer Behauptung über weitere Angriffe veröffentlichten internen Dokumente (Organisationspläne, Dienstanweisungen, Formulare) stammen nicht aus einem erfolgreichen Angriff auf Datennetze oder Server.

7. Wie schätzt die Bundesregierung die Qualität der Maßnahmen in Bezug auf Datenschutz und Datensicherheit auf den betroffenen Servern ein?

Der erfolgreiche Angriff hat Mängel in der Datensicherheit der betroffenen Server aufgezeigt. Welche konkreten Einzelmaßnahmen zur Verbesserung der Datensicherheit erforderlich sind, werden die derzeit noch laufenden Untersuchungen zeigen.

8. Sieht die Bundesregierung einen Zusammenhang zwischen den bekannt gewordenen mangelhaften Sicherheitsvorkehrungen und dem Personaleinsatz bzw. dem Ausbildungsstand der betroffenen IT-Abteilungen und der jeweils Verantwortlichen?

Nach bisherigem Ermittlungsstand gehen die Mängel in der Datensicherheit der betroffenen Server auf individuelles Fehlverhalten zurück. Hinweise auf einen systematischen Zusammenhang zu Personaleinsatz oder Ausbildungsstand haben sich nicht ergeben. Die umfassende Auswertung der derzeit noch laufenden Untersuchungen wird Maßnahmen zur Aus- und Fortbildung sowie zur Personalentwicklung einschließen.

9. Werden eventuell festzustellende mangelnde Sicherheitsvorkehrungen zu dienstlichen Konsequenzen bei den Verantwortlichen führen?

Die Ermittlungen zu den Sicherheitsvorfällen dauern an. Dienstliche Konsequenzen werden geprüft.

10. Welche konkreten Sicherheitsstandards und -prozesse wurden beim Betrieb der betroffenen Server missachtet?

Da die Untersuchungen noch nicht beendet sind, kann hierzu noch nicht abschließend Stellung genommen werden. Nach derzeitigem Erkenntnisstand hat eine Sicherheitslücke im verwendeten Datenbankverwaltungsprogramm das Einschleusen von Schadsoftware und somit den illegalen Zugriff auf die Server ermöglicht.

Der Vorfall wird zum Anlass genommen, die bisherigen Sicherheitskonzepte für die Informations- und Kommunikations-Infrastruktur und deren Umsetzung auf den Prüfstand zu stellen. Dabei sind auch die Sicherheitsstrukturen sowie die Informations- und Meldewege zu überprüfen und gegebenenfalls anzupassen. Über weitergehende Maßnahmen wird nach Abschluss der Schwachstellenanalyse entschieden.

11. Wie lange wurden die Server der Bundespolizei, der Zollverwaltung und der Landeskriminalämter (bitte konkret angeben) in Folge der Angriffe abgeschaltet?

Die beim Bund eingesetzten PATRAS-Zielverfolgungssysteme wurden unverzüglich nach Bekanntwerden des Vorfalls vorsorglich abgeschaltet und die vorhandenen Daten gesichert. Darüber hinaus sind nach Kenntnis der Bundesregierung auch alle anderen PATRAS-Zielverfolgungssysteme abgeschaltet worden. Die Systeme sind derzeit noch abgeschaltet.

12. Welche Aufgaben von Zollverwaltung und Bundespolizei konnten aufgrund der Angriffe wie lange nicht oder nur unzureichend erfüllt werden, und welche Folgen haben die Angriffe für die Aufgabenerfüllung?

Die Ermittlungen mit Zielverfolgung können von Zollverwaltung und Bundespolizei, allerdings mit höherem Aufwand, weitergeführt werden.

13. Welche kurzfristigen Maßnahmen wurden unternommen, um die Sicherheit der kompromittierten Netze und Server wiederherzustellen?

Bei den Sicherheitsbehörden des Bundes wurden mehrere Sofortmaßnahmen durchgeführt, darunter eine sofortige IT-Sicherheitskurzrevision, forensische Untersuchungen der Firewall-Systeme und außerplanmäßige Suchen nach den gefundenen Schadprogrammen bei der gesamten IT-Infrastruktur. Hierbei wurde festgestellt, dass die Angriffe auf die von den übrigen polizeilichen IT-Anwendungen getrennten Zielverfolgungssysteme beschränkt blieben. Die beim Bund eingesetzten PATRAS-Zielverfolgungssysteme wurden außerdem abgeschaltet und die vorhandenen Daten gesichert.

14. Sieht die Bundesregierung einen Zusammenhang zwischen den bekannt gewordenen mangelnden Sicherheitsvorkehrungen und dem in der Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 17/6655 konstatierten Investitionsmehrbedarf von 8 Mio. Euro bei der IT der Bundespolizei?

Zwischen den aktuellen Vorfällen und dem Erfordernis, die vorhandene Ausstattung der Bundespolizei ständig an die Entwicklungen im Bereich der Informations- und Kommunikationstechnik anzupassen, besteht kein Zusammen-

hang. Nach bisherigem Erkenntnisstand lag die Ursache in individuellem Fehlverhalten beim Umgang mit der eingesetzten Technik und nicht in fehlender Technik.

15. Welche Maßnahmen, z. B. zusätzliche Investitionen, Neueinstellungen und Ausbildungsinitiativen, gedenkt die Bundesregierung in Angriff zu nehmen, um die Sicherheit von Datennetzen und Servern von Zoll und Bundespolizei zu verbessern?

Die Informations- und Kommunikations-Infrastruktur der betroffenen Bundesbehörden wird einer umfassenden Sicherheitsüberprüfung unterzogen. Darunter fallen u. a. die Revision der Informationssicherheit, eine Schwachstellenanalyse und Penetrationstests. In einem weiteren Schritt ist vorgesehen, die bisherigen Sicherheitskonzepte für die Informations- und Kommunikations-Infrastruktur und deren Umsetzung auf den Prüfstand zu stellen. Dabei sind auch die Sicherheitsstrukturen sowie die Informations- und Meldewege zu überprüfen und gegebenenfalls anzupassen. Über weitergehende Maßnahmen wird nach Abschluss der Schwachstellenanalyse entschieden.

16. Wann wurde der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und von wem über die Datenlecks informiert?

Nach Erkenntnissen der Bundesregierung hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit am 8. Juli 2011 über Meldungen aus den Medien von dem Angriff erfahren. Die von ihm am gleichen Tag schriftlich an die betroffenen Behörden gerichteten Fragen wurden beantwortet.

17. Ist die Bundesregierung bereit, auch für Bundesbehörden gesetzliche Regelungen anzustreben, die sicherstellen, dass „bei Verlust, Diebstahl oder Missbrauch sensibler personenbezogener Daten (…) unverzüglich die hiervon Betroffenen sowie die Aufsichtsbehörden zu unterrichten (sind)“ (PE BfDI vom 12. Juli 2011)?

    Wenn nein, warum nicht?

Die Frage zielt auf eine Erweiterung der Regelung des § 42a des Bundesdatenschutzgesetzes (BDSG), die eine umfangreiche Informationspflicht für eine nichtöffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 BDSG bei unrechtmäßiger Kenntniserlangung von Daten vorsieht, auf alle öffentlichen Stellen des Bundes. § 42a BDSG ist erst am 1. September 2009 in Kraft getreten. Gemäß § 48 Satz 1 BDSG muss die Bundesregierung dem Bundestag bis zum 31. Dezember 2012 u. a. über die Auswirkungen des § 42a BDSG berichten. Im Hinblick hierauf ist es verfrüht, jetzt bereits Aussagen zu einem eventuellen Änderungsbedarf des § 42a BDSG zu treffen.



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333